INDEPENDENT FORENSIC AUDIT

Biometric Surveillance, Consent Validity, and Procurement Governance in UK Higher Education

A Case Study

Author: Valentina Bozhilova, MIAB

Version: 2 October 2026 (first drafted April 2026; updated as further evidence is obtained)

Version note: This version (2 October 2026) updates Section 20 with the Department for Education's substantive response to the Section 50/HERA 2017 commissioning request referenced in the 6 September 2026 version as outstanding: a refusal under Section 12 of the Freedom of Information Act 2000, and the narrower follow-up request submitted the same day under the Department's own Section 16 advice. The 6 September 2026 version added Part IV (Sections 19–20), covering the sector regulator's own admitted absence of a framework for assessing this category of complaint, and a structural conflict of interest between the sector funding regulator's commissioning and oversight roles. The 18 August 2026 version added Part III (Sections 15–18) and corrected two internal cross-references present in the 31 July 2026 version. See OSF/Archive.org version history for prior versions. This version also harmonises the 2024/2025 deployment chronology, updates the unapproved DPIA duration to 46 months, incorporates Section 173 DPA 2018 regulatory analysis in Section 11, adds architectural evidence from GoTo's published Rescue Administrator Guide in Section 18, and integrates sub-processor AI-training compliance analysis under DfE safety standards in Section 3.

DISCLAIMER & AUTHOR'S NOTE

This independent forensic audit is published strictly for public interest, academic analysis, and educational research purposes. All findings, figures, and statements contained herein are grounded exclusively in statutory Freedom of Information (FOI) disclosures, official institutional records, court filings, and publicly accessible documentation valid as of 2 October 2026. This report reflects independent analytical research and does not constitute formal legal counsel or formal legal advice. References to third-party litigation, vendor performance, or regulatory proceedings accurately reflect cited public dockets and official records and do not assert liability beyond cited sources.

How this case study is built

Part I sets out the findings on the deployment itself, beginning with the Executive Summary below. Part II (Sections 10–14) adds what has come to light since: the University's own written admission of the legal test for when consent is invalid, applied to its own separately-published policy; a reversal in the University's own account of how it handles personal data; the settlement of related litigation in the United States and the litigation that remains unresolved; and the University's own internal IT department's written uncertainty about the platform it deployed. Part III (Sections 15–18) turns from the deployment itself to its governance and procurement context: an unassessed public-record adjacency between a University office-holder and the investment group whose credit division financed the vendor's ultimate owner; the unresolved question of who signed the Meazure contract and under what delegated authority; the absence of any data-protection category in the University's own procurement risk framework; and a narrower, still-live assurance gap in the compliance record of GoTo, the remote-access sub-contractor whose software was used to invigilate the examinations at the centre of this case. Part IV (Sections 19–20) turns to the sector's own regulators: the data protection regulator's own written admission that it holds no framework for assessing this category of complaint, set against its own published sector-wide casework data; and a structural conflict of interest in which the same body that regulates the University's financial viability is also, concurrently, its commissioning funder for a separate national project. The Open University's own written evidence to Parliament's Education Committee (AIE0218, May 2026) is examined in Part II, Section 10; it is public.

PART I — THE DEPLOYMENT

Executive Summary

In September 2024 a major UK university made remote invigilation software (ProctorU, operated by Meazure Learning) mandatory for high-stakes summative assessments. Internal governance documents, obtained under the Freedom of Information Act, reveal that the deployment proceeded despite an unsigned Data Protection Questionnaire (DPQ) containing explicit "DO NOT PROCEED" red-cell warnings, international transfers of biometric data to non-adequate countries, undisclosed sub-processor risks, and a requirement for 16- and 17-year-old students to have a guardian sign a contract with the provider. Two distinct dates recur through this case study and are not interchangeable: September 2024 is when the University's mandate decision took effect and the platform began onboarding students; September 2025 is when the specific mandatory summative examinations this case study examines in closest detail — including the B252 and B253 sittings discussed throughout — were actually

sat. The governance failures documented in Part I predate and span both dates; where a specific month matters to a specific finding, the text below distinguishes the two.

Section 1: The Deployment Decision — Procurement Conflicts and Financial Incentives

In September 2024 the University made ProctorU mandatory for high-stakes summative assessments. The software was procured through the JISC CHEST Framework Agreement Reference 8089. JISC simultaneously operates the UK's National Research and Education Network, administers the procurement framework, and issues cybersecurity advisories for the sector. Institutions meeting utilisation metrics received a $10,000 fee waiver incentive. This created a direct financial conflict between maximising adoption and objectively assessing platform risks.

At the time of deployment, three major institutions — ACCA, the British Council, and the University of London — had already exited the platform for security and integrity reasons. The University proceeded regardless.

On 26 February 2026 JISC published a news release summarising its annual cyber threat intelligence report (the full report itself restricted to its members' cyber security community group), confirming total incidents against UK education and research rose from over 11,000 to over 16,000 in 2025, with a companion cyber posture survey the same day naming ransomware and phishing as the sector's top threats and flagging AI-enabled attacks as an emerging concern. Separately, LogMeIn — a remote-access tool associated with the ProctorU platform's technical operation — is the subject of a documented HIGH/HIGH-classified security advisory (NCC-CSIRT-2025-025, Nigeria Communications Commission CSIRT) identifying it as actively abused by threat actors to disguise malware as legitimate remote-access software and establish persistent backdoor access. That advisory concerns LogMeIn/GoTo Resolve — a separate GoTo remote-access product from LogMeIn Rescue, the product actually deployed for invigilation and examined on its own compliance record in Part III, Section 18. This is cited here as independent, dated sector-context corroboration that the class of tool involved carries a documented high-severity abuse profile, not as a finding about Rescue specifically. The financial conflict identified above — the same body administering procurement and receiving a utilisation-linked fee waiver — stands independently of this advisory and does not depend on it.

On 11 March 2026 (Los Angeles Superior Court) — while students at the University were sitting mandatory ProctorU examinations — the State Bar of California filed an amended complaint against Meazure Learning. The amended complaint was filed after receiving Meazure Learning's own internal documents through discovery. The State Bar's amended complaint

opens: “Meazure sold competence but delivered chaos.” The complaint documents that even as Meazure Learning externally pitched its capabilities, it internally questioned its ability to deliver. The amended complaint includes claims for fraud, negligent misrepresentation, and breach of contract, and seeks punitive damages. The State Bar confirmed that Meazure Learning deliberately concealed information and that its deception and delay tactics concealed the true nature and extent of its failures. These internal documents confirm that Meazure Learning was making false promises it knew it could not deliver — in September 2024, the exact month the University made ProctorU mandatory for its students.

Section 2: Biometric Data Collection — No Equivalent Protection to Financial Services

Open a banking app and the biometric checks are regulated, time-limited, and reviewable by a human if something goes wrong. Sit a University exam through ProctorU and none of that applies. Every examination session, according to documents released under FOI, ProctorU collects:

- Facial recognition — continuous throughout the examination
- Eye-movement tracking — continuous
- Voice recording and analysis — continuous
- Keystroke dynamics — continuous
- Screen recording — continuous
- Hardware profiling: CPU model, processor cores, RAM capacity, monitor resolution, graphics card, network card MAC address
- Network profiling: IP address, upload/download speed, ISP information
- Software environment: operating system version, browser type, installed extensions, device fingerprint
- Multiple facial photographs stored for identity verification

None of the hardware, network, or software environment data serves any purpose related to examination integrity, in direct conflict with the UK GDPR data minimisation principle under Article 5(1)(c).

Students subject to ProctorU receive none of the protections that apply to biometric authentication in financial services — FCA regulation, Strong Customer Authentication requirements, mandatory human review of automated decisions, or strict regulated retention limits. The University’s own DPQ confirms full examination video and audio is retained for three

years, while students are routinely told data is kept for approximately seven days. The same document admits that “part of a DSAR cannot be met” — the University cannot fully comply with its legal obligation under UK GDPR Article 15 because the data has been designed to be unreachable.

The DPQ denies the use of artificial intelligence. The 2023 CHEST procurement contract explicitly describes “machine-learning algorithms” to detect “aberrant behaviour”. One of these statements is false.

This contradiction has deepened following the acquisition of OP360 by iQor CXBPO on 5 January 2026. iQor’s infinityAiQ platform, launched in 2025, processes over 2.7 billion tokens weekly using large language models. Student biometric examination data now flows through a sub-processor operating an AI-first platform at industrial scale. The University’s own DPQ continues to deny the use of artificial intelligence.

ProctorU is marketed and operated as live proctoring, and the examination is also continuously recorded on video and audio throughout (Section 2, above). Two separate review mechanisms therefore exist, not one: a human proctor watching in real time — often monitoring several students’ sessions simultaneously — and the recording itself, which may be reviewed after the fact by a proctor, by University staff investigating a specific incident, or not reviewed at all unless a complaint is raised. Neither of those is the same question as whether the automated “aberrant behaviour” scoring the CHEST contract itself describes — the machine-learning layer that flags a session for review or escalation — is itself independently checked by a human before that flag is acted on, or whether it simply feeds a proctor’s real-time judgement or a later recording review without disclosed weight or process. Under UK GDPR Article 22, the right not to be subject to solely automated decision-making with significant effects turns on that distinction, not on whether a human is present in the room or a recording exists somewhere. Neither the DPQ nor any governance document disclosed to date specifies how the automated flag, the live proctor’s own observation, and any later recording review are weighted against each other, or which one determines the outcome recorded against a student.

Section 3: Sub-Processor Risk and Supply Chain Opacity

UK GDPR Article 28 requires data controllers to conduct due diligence on sub-processors and to ensure sub-processing agreements provide equivalent data protection guarantees. Article 28(2) requires prior written authorisation before a processor engages a new sub-processor.

Follow the sub-processor chain for ProctorU, documented in FOI responses, and the compliance failures are not isolated. They stack.

Radius Global Solutions — a former sub-processor — suffered a data breach in June 2023 in which the Clop ransomware gang exposed 632,204 records

through the MOVEit vulnerability. This breach was not disclosed to students. The University substituted Radius after the matter was raised in correspondence — a reactive response, not a proactive safeguarding measure. A named university official confirmed in writing that student exam data was permanently lost. Active class action litigation against Radius Global Solutions following this breach remains ongoing.

On 5 January 2026, OP360 — a current sub-processor in the ProctorU chain — was acquired by iQor CXBPO. This acquisition expanded iQor's global delivery presence across six countries. No student notification was issued. No Article 28(2) prior authorisation was documented. The six countries of operation and their UK GDPR adequacy status are set out below:

Country	UK GDPR Adequacy Status
Philippines	No UK adequacy decision
India	No UK adequacy decision
Colombia	No UK adequacy decision
Trinidad	No UK adequacy decision
Egypt	No UK adequacy decision
United States	No UK adequacy decision (limited frameworks only — not automatically applicable to all transfers)

Source: iQor press release, GlobeNewswire, 5 January 2026. UK adequacy decisions: UK Government adequacy decisions register.

None of these six countries holds a UK adequacy decision. Under UK GDPR Article 44, transfers of personal data to third countries may only take place if the conditions in Chapter V are met. No such conditions were disclosed to students at any point. The University's own DPQ confirms: "India and the Philippines access the servers from their respective countries." This confirmation appears in a document that was never signed and carries an explicit DO NOT PROCEED directive — meaning the international data transfers were identified as a compliance risk before processing began, and processing proceeded anyway.

A separate disclosure sits alongside this sub-processor chain, concerning a different vendor in it. Students raise Subject Access Requests and technical complaints with ProctorU through its chat-based customer support channel, which Meazure Learning's own Privacy Policy (current version, last updated 6 May 2026) discloses is run through Zendesk. The policy states: "Information you provide through our chat features (including the content of your messages) may be processed by Zendesk's AI tools to facilitate and improve our support interactions. Your interaction data may be used by Zendesk in accordance with their Privacy Notice to help train and improve

Zendesk's AI systems." This sits against a standard published by the Department for Education for exactly the sector Meazure Learning supplies into. The DfE's "Generative AI: product safety standards," published 19 January 2026 and addressed to "edtech developers and suppliers to schools and colleges," states that such products should "not collect, store, share or use personal data for any commercial purposes, including further model training and fine-tuning, without confirmation of appropriate lawful basis." No lawful basis for using students' support-chat content — raised, in part, to pursue their own data protection rights — to train a third party's AI systems is disclosed anywhere in the materials provided to students. The DfE standard is sector guidance, not law, and does not itself bind Meazure Learning or the University; it is cited here as the sector's own benchmark for the practice Meazure Learning's Privacy Policy discloses, not as a finding that either body has breached it.

Section 4: Governance Failure — The DO NOT PROCEED Problem

Under UK GDPR Article 35, a Data Protection Impact Assessment (DPIA) is mandatory before processing that is likely to result in a high risk to individuals. Remote invigilation meets multiple high-risk criteria: systematic monitoring, biometric data, processing on a large scale, vulnerable data subjects, innovative technology, location tracking, and risk of physical harm in a security breach. The document discussed throughout this case study as the Data Protection Questionnaire (DPQ) is the same document: the University's own Information Rights team confirmed in writing that "DPQ is the name used for DPIAs at the OU" (FOI2025/238, Daniel Webb, Senior Manager Information Rights). "DPQ" and "DPIA" are therefore used interchangeably below to refer to the single document described here, consistent with the University's own terminology.

The University began this Data Protection Impact Assessment for ProctorU in December 2022. The document remains version 0.9, unsigned after 46 months of continuous processing, and contains the explicit instruction: "If any cells are coloured red, please do not proceed with your activity until you have received authorisation." Multiple cells were coloured red. Processing proceeded. The ICO was never consulted. The DPIA remains unsigned to this day.

An updated version was produced in March 2026 — during active OIA proceedings, active FOI scrutiny, and active discrimination complaint handling. It remains version 0.9. It remains unsigned. The DO NOT PROCEED directives remain present.

The document's own conclusions, not an outside reading of it, already record this as unresolved. Its Assessment tab records the Individual Rights requirement as met in general terms, then immediately qualifies that:

because biometric data is destroyed after seven days, the right to withdraw consent and the right to data portability are recorded as only “partially met.” The same tab separately records the organisation’s own Security control — a backup process for the application — as only “partially met” too, because the backup process “has been created, but not tested.” This is the University’s own compliance function, in the same governance document, declining to record full compliance against the obligations the DPIA exists to verify.

The same Assessment tab also contradicts the document’s own AI/ML tab. Q23 of the Questionnaire tab, and the AI/ML tab it triggers, confirm that the platform processes a student’s own webcam image to verify identity — the AI/ML tab’s own description states the system “looks at a picture from the student’s webcamera prior to exam and during the exam looks if the person looks similar to the reference picture taken,” and separately describes voice similarity matching. The Assessment tab, completed from the same questionnaire, nonetheless records: “Artificial Intelligence, Machine Learning or Algorithms usage are not part of this activity, therefore this requirement has been met,” and, separately, “Profiling or automated decisions are not part of this activity, therefore this requirement has been met.” The same document that describes continuous AI-driven facial and voice matching against a reference image, elsewhere in the same document, certifies that no AI, machine learning, or automated decision-making is involved at all.

In November 2025 a senior university official confirmed in writing: “We are not fully compliant with data protection law.” This admission was made while mandatory biometric data collection from thousands of students was ongoing.

A Freedom of Information response dated 26 March 2026 — FOI2026/039 — confirmed that the University has never obtained an independent SOC 2 Type II security audit report for Meazure Learning. The University’s own response states: “A SOC 2 attestation report was not obtained as part of this process” and “We do not currently ask for SOC 2 attestation reports as part of this process.” The University’s assessment of Meazure Learning’s security posture was conducted through an internal questionnaire in early 2024 and two unnamed continuous cyber security risk rating services. No independent auditor was engaged. No Bridge Letter or Letter of Attestation was obtained for 2024 or 2025. The University mandated biometric data collection from thousands of students on a platform whose independent security compliance was never verified by a qualified auditor.

This constitutes a documented circular compliance failure. The DPQ drafted in December 2022 cited SOC 2 as the security basis before the certification existed. Meazure Learning announced SOC 2 Type II certification in January 2023 — at which point an independent audit report became publicly

available and obtainable. The University conducted a formal procurement assessment of Meazure Learning in early 2024 and still did not request the report. Live biometric processing of students began in September 2025. The FOI response of 26 March 2026 confirms the report was never obtained and is not asked for. On the same date, the University released its updated DPQ — which continues to record the security requirement as “met” on the basis of SOC 2, citing “SOC 2 Type II certification details in the contract.” The document asserting compliance and the process that was supposed to produce that compliance describe entirely different things. The two unnamed commercial risk rating services cited as the operative assurance mechanism assess external-facing technical posture — open ports, SSL configuration, and network health — and do not assess internal data handling, retention practices, sub-processor compliance, or cross-border transfer safeguards. They are not a substitute for the independent audit the DPIA records as the basis for compliance.

The structural failure documented in this case study — a DPIA recording a SOC 2 certification as its security basis without the University ever obtaining or reviewing the underlying report — has been independently validated by a sector-wide scandal that broke in March 2026. An investigation published on 19 March 2026 by an anonymous whistleblower writing as “DeepDelver” and reported by TechCrunch on 21 March 2026 documented that Delve, a Y Combinator-backed compliance automation startup valued at $300 million, allegedly produced 494 near-identical SOC 2 reports with auditor conclusions written before evidence was reviewed. In 99.8% of reports, Section 3 — which is supposed to describe each company’s specific security programme — contained identical text including the same grammatical errors and nonsensical descriptions regardless of each client’s size, industry, or technical architecture. One recurring error — the phrase “because there no security incidents,” with the same missing word — appeared identically across hundreds of reports, making independent authorship statistically and professionally impossible. Every single SOC 2 Type II report in the dataset recorded zero security incidents across all 259 companies over multi-month observation periods — a statistical impossibility. The auditor’s conclusions existed in draft reports before clients had provided their company description, network diagrams, or signatures — directly violating AICPA AT-C Section 205, which requires practitioners to form conclusions based on their own independent examination. DeepDelver described the structural consequence in terms that apply with equal force to the University’s own position: “By generating auditor conclusions, test procedures, and final reports before any independent review occurs, Delve places itself in the role of both implementer and examiner. This is not a technicality. It is a structural fraud that invalidates the entire attestation.” The University’s DPQ recorded SOC 2 as met — placing itself in the role of examiner — without ever obtaining the report that would have constituted independent review. The primary

auditors — Accorp, Gradient Certification, Glocert, and DKPC — were alleged to be operated by junior teams in India rather than experienced US-based CPAs, using US shell companies and mailbox addresses, frequently in Montana, to appear as domestic accredited firms. The alleged workflow inverted the audit process entirely: Delve allegedly generated the final conclusions itself using internal templates and sent them to these Indian firms for rubber-stamping — the conclusions travelled from the platform to the auditor, not the other way around. The investigation was not uncovered by the SEC, the AICPA, or any compliance oversight organisation. It was uncovered by a whistleblower publishing anonymously on Substack. No regulator flagged 494 allegedly identical reports. This scandal has publicly confirmed what the University's own FOI response demonstrates in this specific case: a SOC 2 certification is meaningless without independent verification of the auditor's identity, the scope of the audit, and the methodology applied. The University cannot provide any of those three things for the certification it records as the basis for its security compliance determination. Bryan Geels, Partner at GN (a Smith + Howard Company), stated publicly in response to the Delve scandal: "SOC 2 is not software. It is an attestation that depends on management representations, auditor independence, and adherence to professional standards. Automation platforms are tools. They do not transfer accountability away from management." That principle applies directly to the University's position. Accepting a SOC 2 claim without obtaining the underlying report is a management decision. Switching EdTech platforms does not absolve it. The depth of the structural failure has been further documented by Taylor Gavigan, CPA, CISA, a named professional in internal control and risk advisory who was engaged as a SOC specialist on the AICPA peer review of one of the implicated audit firms and subsequently dismissed after reporting his findings. Gavigan disclosed publicly on LinkedIn that the audit files he reviewed showed engagement fees of between $1,200 and $1,500 per audit — a fraction of the $15,000–$50,000 a legitimate SOC 2 Type II engagement costs — with no workpapers outlining testing procedures, no documentation of observations, no inspection of documents, and no inquiry of personnel. The AICPA framework produces identical-looking reports regardless of audit quality or cost — a $1,500 rubber-stamp audit and an $80,000 rigorous engagement both result in the same SOC 2 Type II logo. The only mechanism to distinguish them is the underlying report. The University never obtained it. The assertion and management representation letter had been signed by the auditor rather than by management, as required. The control testing methodology consisted of generic placeholder language. When Gavigan communicated these findings to firm management, he was dismissed without payment. He stated: "The Delve situation is merely scratching the surface" — noting that the engagements he reviewed involved another well-known, internationally-based platform beyond Delve. It should be noted that this testimony comes from a credentialled professional who attempted to use the AICPA's own peer review mechanism

to flag the failure — and was removed for doing so. The mechanism designed to catch rubber-stamping actively suppressed the professional who identified it. The University's own DPQ exhibits the same pathology in the opposite direction. The Delve reports were mass-produced with identical content because auditors were not independently assessing each company — they were applying a template. The University's DPQ was completed to satisfy a process, not to assess a risk. Question 25 states "picture is translated to a score, picture is not stored" — a generic answer that remained unchanged in the March 2026 update even after the same document disclosed that eye colour is collected as biometric data and that the first SAR could not be fulfilled without routing student data through a personal OneDrive account outside the contracted system. Both documents — the Delve SOC 2 reports and the University's DPQ — were produced to close a compliance gate, not to open a compliance process. The structural vulnerability this represents was documented by a credentialled practitioner before the scandal broke. Juan Carlos Munera, a Qualified Security Assessor (QSA), published an analysis on 8 March 2026 — eleven days before DeepDelver's investigation and eighteen days before the OU's FOI response confirmed the SOC 2 report was never obtained — warning that compliance automation platforms were producing packages that looked indistinguishable from organisations with mature security programmes. Writing from the assessor side, Munera described the operational reality: "A SOC 2 report arrives, it gets filed, it satisfies a procurement requirement, and nobody reads past the opinion letter." He posed the question that the Delve scandal then made impossible to avoid: "How would we know if a vendor's compliance report was fabricated? The honest answer for most organisations is that they wouldn't." That answer describes exactly the University's position. The FOI response of 26 March 2026 confirmed they would not know — because they never obtained the report. No link between Meazure Learning and Delve specifically is alleged; the Delve scandal and associated testimony are cited as sector-wide evidence of the structural vulnerability that the University's own procurement failure has left unaddressed.

It is worth considering the University's institutional knowledge in this context. The University's Business School launched its BSc (Hons) Accounting and Finance degree in October 2022, specifically designed to grant graduates up to eight CIMA exam exemptions under its AICPA & CIMA accreditation. The University has accepted CIMA professional qualifications for credit transfer for years, and in late 2025 reached new formal accreditation milestones, including recognition from the Institute of Chartered Accountants of Scotland, alongside its established AICPA & CIMA-accredited status. AICPA & CIMA is the body that both provides the professional qualifications the University markets to students and governs the SOC 2 standard the University cited as the security basis for mandatory biometric processing of those same students. Two months after launching

that degree — in December 2022 — the University produced the DPQ that cited SOC 2 as met. The report that would verify that claim was never obtained. The University's own Accounting and Finance faculty teach the governance and assurance frameworks that SOC 2 is designed to reflect. The University is not an institution unfamiliar with what an auditor's report is, what it contains, or why it is the only mechanism by which a SOC 2 claim can be independently verified. There is no public registry of SOC 2 certifications. Unlike ISO certifications, the AICPA maintains no public database of certified organisations. The auditor's report is the only verification mechanism that exists. The OU did not use it. The Delve investigation documented a further structural vulnerability: certification mills allegedly exploited specific state law loopholes — notably in Montana — that allow international entities to hold a US-based CPA licence without physical presence, enabling Indian operations to present as US-based audit firms to enterprise clients conducting due diligence. The University had no mechanism to detect this, because it never requested the report that would have identified the auditor. Against that background, the FOI response confirming that no SOC 2 report was ever obtained — and that the University does not ask for such reports as part of its process — requires explanation that goes beyond administrative oversight. Three explanations are possible: the University did not ask; the University asked and Meazure Learning declined to provide the report; or the University understood that citing SOC 2 in the DPQ would satisfy an internal compliance process that would not require the underlying document. None of these explanations is compatible with adequate governance of mandatory biometric data collection from thousands of students by an institution with the University's level of professional familiarity with the standard it failed to verify. Industry guidance confirms that a fraudulently obtained certification provides zero legal protection under GDPR and may increase regulatory penalties where the relying institution had the professional knowledge to identify the red flags of a certification mill but did not verify the underlying report. The circular structure of this arrangement — in which the same body accredits the degree, governs the security standard, and licenses the auditors whose independence has been called into question — is not a coincidence of institutional geography. It is the assurance architecture that UK higher education has built around EdTech procurement. Whether that architecture is adequate is precisely the question this case study puts on the record.

The second assurance mechanism cited by the University — SecurityScorecard — has been independently confirmed as non-functional for this purpose since before the September 2025 exam sittings began. SecurityScorecard's own platform documentation confirms that Public Scorecards were fully deprecated on 27 August 2025 — three weeks before mandatory biometric processing commenced. The previously public-facing view of scorecards, accessible at scores.securityscorecard.io, is no longer available to the general public. SecurityScorecard's own support

documentation states that the supported replacement is a Trust Centre, and identifies the only remaining option for external parties as: “Ask Meazure Learning to share their Trust Centre link with you.” Meazure Learning has not set up a Trust Centre. This means that from 27 August 2025 onwards, the sole publicly accessible SecurityScorecard assurance signal for Meazure Learning has been a badge on Meazure Learning’s own compliance page that links to a deprecated system. The underlying score data is not publicly accessible without a paid SecurityScorecard Business account with API credentials. The University’s described “continuous” monitoring of SecurityScorecard therefore rests on either a dead public badge — which ceased to reflect live data before the first exam session — or an undisclosed paid subscription that has never been referenced in any governance document released to date. Either way, the assurance mechanism the University cited in its FOI response of 26 March 2026 was already non-functional at the point of deployment. The University mandated biometric data collection from hundreds of students on a platform for which no functioning independent security assurance existed.

A comparison of the original DPQ (referred to in this case study as GOV-1, obtainable in full via the FOI link in the references section; the document was released after September 2025) with the updated DPQ released via FOI2026/039 (March 2026) reveals that the updated document introduced new admissions that directly contradict the questionnaire answers still sitting above them. The updated Risk Assessment tab discloses that AV recordings are retained for 12 months then held in cold storage for a further 24 months — a total of up to 36 months — while the questionnaire answers continue to state “7 days for identification, 3 years invigilation audio and camera” and Q25 continues to state “picture is translated to a score, picture is not stored.” The updated document lists eye colour as a category of biometric data — a category never disclosed to students. It admits that students cannot exercise Subject Access Rights directly in ProctorU, and that the first SAR processed required the University to route student biometric data through a personal OneDrive account — outside the contracted system. The DPQ author describes this process as “very slow” — their own words, in the governance document that records data subject rights as a met requirement. It discloses that ProctorU uses a third-party tool allowing remote cursor and keyboard control of student devices. None of these admissions are reflected in the questionnaire answers, the privacy notice given to students, or the University’s public communications. The document remains version 0.9. It remains unsigned. The sign-off table shows one entry dated 6 December 2022, with no approver and no review date. The Q42 Information Asset Register field continues to read: “Link don’t work.” This should not be read as a typographical error. It is, in four words, an accurate description of the institution’s entire governance framework: the links between policy and practice do not work, the links between documentation and implementation do not work, and the links

between stated compliance and verified compliance do not work. The broken hyperlink was not fixed in the March 2026 update. It has not been fixed in 46 months of continuous processing.

The Government Cyber Action Plan, updated January 2026, identifies cyber risk to the public sector as critically high and sets clear requirements for arm's length bodies — including universities incorporated by Royal Charter — covering asset management, protective monitoring, and incident response. The University's documented failures represent precisely the foundational vulnerabilities the plan identifies as systemic.

Section 4A: Vendor Compliance Misrepresentation — The Assurance Chain Examined

This case study examines the compliance representations made by Meazure Learning on its public-facing compliance page at meazurelearning.com/compliance, which constitutes the primary assurance document available to institutions conducting due diligence on ProctorU. It is the document a responsible procurement officer would consult to verify the platform's claimed compliance status. An examination of that page against independently verifiable sources reveals systematic misrepresentation across four distinct assurance categories.

SOC 2 Type II. The compliance page asserts that Meazure Learning is SOC 2 Type II certified, having undergone an extensive third-party audit. Section 4, above, already establishes that no such report was ever obtained or requested by the University. What the compliance page adds is a fresh angle on the same failure: it names no auditor. Meazure Learning does not publicly name the CPA firm that issued their SOC 2 opinion. Legitimate top-tier SOC 2 auditors — such as Schellman or BDO — are routinely named by certified organisations as a point of professional pride. Concealing the auditor's identity was a core tactic of the certification mills exposed in the Delve scandal, where Indian operations used NDAs to prevent clients from discovering that the signing CPA was a junior team behind a Montana shell company. Because the University never obtained the report, it has never seen the auditor's name. FOI2026/039 asked the University directly for the name of the independent CPA firm that issued the most recent SOC 2 opinion held for Meazure Learning. The University's statutory response was unambiguous: "This information is not held." The University does not know who audited the platform processing biometric data from thousands of its students. The AICPA SOC 2 logo displayed on the compliance page is a trademarked badge that per AICPA's own published logo guidelines may only be used by organisations with a valid SOC 2 report signed by a licensed CPA firm. If no valid independent report exists — or if the report was issued by one of the certification mills implicated in the Delve scandal — displaying the logo constitutes a potential violation of AICPA trademark and professional standards. The Open University, as an AICPA & CIMA

accredited institution, would be expected to know those rules. It did not ask for the document that would verify compliance with them. The AICPA is itself currently seeking public comment on proposed changes to its attestation standards — as of February 2026 — specifically to prevent offshore junior teams from performing audits without US-based CPA oversight. The regulator is acknowledging the structural failure in real time. The University's DPQ continues to record the existing standard as met.

SecurityScorecard. The compliance page displays a SecurityScorecard badge as evidence of ongoing cybersecurity assurance. Section 4, above, already establishes that this badge linked to a system deprecated on 27 August 2025 — three weeks before the exam sittings it was meant to assure — and that no functioning replacement was ever set up. The point specific to the compliance page itself: it displays that badge as live assurance to any procurement officer who visits it, with nothing on the page itself disclosing that the underlying system has been dead since before the badge was last relevant to a live decision.

1EdTech Certification. The compliance page references IMS Global Data Privacy Certification and links to a ProctorU certification profile. The 1EdTech TrustEd Apps Directory confirms as of March 2026 that the current ProctorU product has no active certifications and that ProctorU is not a member of 1EdTech. The sole certified entry in the directory is ProctorU v2020 — a product version from 2020. The current Meazure Learning products (Examity and ExamityProctoringTool) likewise carry no active certifications. The directory states explicitly: "If a product is NOT listed here it has either not passed 1EdTech testing or its certification has expired." Furthermore, the vetting review for the ProctorU profile discloses that one of the three reviewers was Cory Clark, Director of Quality and Process Improvement at Meazure Learning — the vendor whose product was being assessed. The remaining reviews were conducted by Kevin Lewis, Data Privacy Officer at 1EdTech. No independent external auditor contributed to the review. The assurance framework for the product deployed to UK university students processing special category biometric data therefore rests, in part, on vendor self-assessment.

GDPR Legal Misattribution. The GDPR section of the compliance page displays a GDPR compliance logo that links directly to EUR-Lex CELEX reference 32018R1725. That instrument is Regulation (EU) 2018/1725 — the data protection regulation governing EU institutions and bodies in their own internal processing activities. It has no application to private commercial processors. The operative GDPR instrument applicable to commercial processors is CELEX 32016R0679 (Regulation (EU) 2016/679). A EUR-Lex search for the linked instrument in the context of obligations on private commercial processors returns no results, because no such obligation exists under that instrument. Meazure Learning's compliance page therefore attributes its GDPR compliance to legislation that does not

govern it. This misattribution would not be detected by a procurement officer following the link, as the EUR-Lex page would display a genuine EU regulation — simply not the one applicable to Meazure Learning's processing activities.

Taken together, these four findings reveal that the compliance page on which institutional procurement decisions were based contained a SOC 2 claim never verified by the procuring institution, a deprecated security badge, a certification that expired or lapsed for the current product version, and a GDPR compliance attribution linking to the wrong EU regulation. No independently verifiable assurance existed for the processing of biometric data belonging to Open University students at the time of the September 2025 examinations. The cumulative effect is that the due diligence ecosystem for EdTech procurement in UK higher education permitted a platform to be mandated for high-stakes biometric assessment without any functioning external verification of its compliance claims.

Section 5: Disability Alternatives Systematically Withheld

The alternative existed. It was granted — to every disabled student who formally asked for it. It was withheld from everyone else, who were told none existed at all. FOI2026/023 confirms it: Teams-based invigilation was granted in every recorded case where a disabled student requested it, for the exact modules and sittings other students were told had no alternative. Knowledge of disability triggers the duty to adjust under Equality Act 2010 Section 20 — not a formal request. Non-completion rates on the affected modules ran as high as 35 percent.

The University's own numbers on this don't even agree with each other. FOI2026/023 put September 2025 registration for B252 at 228 students. FOI2026/044 put the entire presentation's total at 224 — lower than the September figure alone. Two statutory responses, two different counts, no explanation.

A separate FOI response, FOI2026/083, explains why the University cannot readily resolve a discrepancy like this one. Asked whether it holds any internal record of ProctorU examination sittings independent of the live third-party system, the University confirmed it holds "no internal records of the proctoring of the examinations… independent of the live systems held by that provider on their platform ProctorU." The University's own explanation for a related one-student sittings discrepancy between FOI2026/023 and FOI2026/044 — that a student's status in ProctorU's system "may have moved from fulfilled (completed) status to cancelled" after the fact — is only possible because no fixed, independent internal record exists to check it against. The registration-figure discrepancy above is not a transcription error on the University's part that an underlying

master record would resolve. On the University's own account, no such master record exists.

A named case corroborates the statistics. In a letter dated 22 March 2026, the University's own Student Casework Manager, Richard English, confirmed to another OU student that, "on the basis of your pre-evidenced medical needs, it has been exceptionally agreed to offer you an alternative assessment method" for the same module, MST125, that the University's public Help Centre lists as having no alternative to ProctorU. The letter was approved through the University's own Tuition, Assessment, Curriculum and Quality (TACQ) function — the body responsible for assessment delivery — not an ad hoc exception outside the ordinary chain of authority. The student concerned has separately confirmed the arrangement remains in place and is now under way in the current October 2026 presentation, more than six months after the letter was issued — not a historical exception but an active, ongoing accommodation operating in parallel with the University's public position that no alternative exists. He has also stated publicly that he considers FOI2026/023's own count of such grants to be an undercount, and has separately asked the University to clarify it — a live, unresolved question about the disclosed figure, not a settled one. The word the University's own letter uses for this accommodation is "exceptionally." A named, TACQ-approved exception granted on request, and never disclosed as a general policy, is precisely the pattern FOI2026/023's statistics describe.

Section 6: The Safeguarding Gap — Domestic Examination Environments and Children

An examination centre exists to keep the exam controlled and the student safe. Remote invigilation removes both. Students sit high-stakes examinations alone in their own homes, under continuous camera surveillance, with a remote technician holding administrative access to their device. The domestic environment is beyond the institution's direct control and may expose students to risks that examination centres are specifically designed to prevent, including coercive control, domestic abuse, and interference by household members.

Asked directly whether it had assessed these safeguarding risks, the University has not answered.

The University's own DPQ contains a requirement that has never been disclosed to students or parents:

"We have some students who are 16 or 17; they must have a guardian (18+) sign the agreement with the service provider, and be in the room with them during the migration."

A child aged 16 or 17 is required to have a parent sign a contract with a US surveillance company and remain physically present during the examination. No parent was ever informed of this requirement. Under the Consumer Rights Act 2015, information provided after the contract is formed is not binding unless explicitly agreed. This requirement was never disclosed and never agreed.

The Open University has 199,475 students including students as young as 16. This undisclosed parental requirement — buried in an unsigned internal document — has never appeared in any module description, student communication, or published policy.

Section 7: The Enforcement Vacuum — Regulators Without Teeth

The Information Commissioner's Office is the designated data protection regulator with powers to fine, issue enforcement notices, and compel compliance. In November 2025, more than 70 civil society organisations — including the Open Rights Group, Big Brother Watch, Foxglove, and the Good Law Project — wrote to the Science, Innovation and Technology Committee demanding an inquiry into the ICO for collapse in enforcement activity in the public sector. According to the ICO's own review, reported public sector data breaches grew by 11 percent after the regulator adopted its softer approach to public bodies. Data protection complaints rose by 8 percent over the same period.

Neither side of the breach-notification transaction verifies anything. Section 11, below, shows the University could produce no written Article 33 threshold assessment for its own April 2026 phishing breach. A parallel FOI request asked the ICO — the body receiving that same notification — what it does to check it. The ICO's own internal review response, dated 31 July 2026, answers three questions in nearly identical terms. Does the ICO record an outcome category when it first assesses a breach notification? "The ICO does not record a category at the time of its initial assessment. Therefore this information is not held." Does it verify the accuracy of what it is told? "This is not recorded. Therefore it is not held." Does it track any follow-up on accuracy or completeness? "This is not recorded. Therefore it is not held." The internal review upheld all three answers without engaging their substance: "The initial response was clear and accurate." A regulator that does not categorise, verify, or follow up on what it receives is not reviewing notifications. It is filing them.

The gap is sharper set against the ICO's own published standard for what a breach risk assessment should look like. The ICO's own guidance, "Understanding and assessing risk in personal data breaches," instructs organisations that discover a breach to work through seven documented steps: confirm personal information is involved, establish exactly what was

breached, consider who might now hold it, work out how many people are affected, assess how seriously it will affect them, document everything else known about the breach, and only then assess the overall risk — with each step recorded as the investigation develops. This is the standard the ICO asks every controller in the country to apply and be able to evidence. It is not the standard the ICO applied to its own receipt of the University's notification. No category recorded at initial assessment. No verification steps recorded. No follow-up recorded. The regulator publishes a seven-step documented methodology for others and confirms, in the same case, that no equivalent record exists for its own intake of a notification concerning 16,615 affected students.

Section 8: Regulatory Architecture Failure — No Body With Cross-Cutting Remit

No single body has both the remit and the enforcement power to address the intersection of EdTech governance failure, biometric data mishandling, disability discrimination, financial irregularity, and contractual breach that this case represents.

The Office of the Independent Adjudicator (OIA) is the designated higher education complaints body. It is funded by universities. It cannot fine. It cannot compel. It can recommend. Its complaint submission portal operates through a single-use authentication system with no persistent login and no accessible fallback. The OIA's own annual reports document that login failures are a recurring and known problem — dedicated help pages exist for authentication difficulties — yet the system has not been made accessible. This is not a peripheral technical issue. It is a structural barrier to redress for the students most likely to need it.

The Office for Students requires exhaustion of the OIA process before it will act on individual complaints — gated behind a body that is toothless by design and inaccessible by documented system failure.

The Student Loans Company Investigations Team deflected a formal fraud report — documenting 1,665 students registered past the liability point with no recorded outcome — to its complaints team, removing it from the function with authority to flag payments.

The Higher Education Freedom of Speech Act 2023 secure duty came into force on 1 August 2025. Individual enforcement through the courts remains unaffordable following ministerial amendments removing financial support for litigation. The free speech complaints scheme has no announced start date.

The regulatory gap extends beyond domestic complaints infrastructure to the certification ecosystem underpinning EdTech procurement. The failures set out in Sections 4 and 4A point to a jurisdictional gap, not just a

compliance one: no single UK body has authority over the firms issuing SOC 2 certifications relied upon by UK universities. The AICPA treats failed peer reviews as a private matter. The United Kingdom Accreditation Service (UKAS) — the sole national body for accrediting certification firms — only has authority over bodies that seek its accreditation; firms that issue certificates without UKAS accreditation operate legally but outside its oversight. The Financial Reporting Council and the Institute of Chartered Accountants in England and Wales have authority over statutory auditors, not US-linked compliance certification consultants. Certification mills of the kind documented in Sections 4 and 4A — some of which claim UK and European operations — therefore face no UK regulatory consequence for their activities in the EdTech procurement market.

The UK Government's Fraud Strategy 2026–2029, published on 9 March 2026, introduces a directly relevant enforcement framework. Under the Economic Crime and Corporate Transparency Act 2023, large organisations are now liable if they fail to prevent fraud by associated persons. The Open University is a large organisation. Meazure Learning is an associated person for the purposes of the platform the University mandated for high-stakes assessment. If Meazure Learning's SOC 2 certification is found to have been issued by a certification mill operating fraudulently, the University's failure to verify that certification — despite its institutional knowledge of the AICPA standard — is directly relevant to that liability framework. The Fraud Strategy also announces a new Online Crime Centre launching in April 2026, with a £31 million mandate specifically targeting organised fraud infrastructure, including fraudulent online assets and scam networks. The compliance page misrepresentations documented in Section 4A of this case study — a deprecated security badge, a wrong EU regulation, a lapsed certification, and an unverified SOC 2 claim — constitute precisely the category of fraudulent online infrastructure the new Centre is designed to address.

It should be noted that the legislative and enforcement architecture to act on these failures is now in place. What is absent is a designated body with the remit to connect EdTech procurement failures to that architecture.

Section 9: Internal Governance Frameworks — Policy Without Enforcement

The University maintains comprehensive internal governance frameworks covering risk management, data protection, safeguarding, advocacy, and assessment. All are Council-approved, regularly updated, and publicly available. None of these frameworks prevented the failures documented in this case study.

The Risk Management Policy was updated in November 2025 — while the unsigned DPIA was still active, while the breach log had been closed

without ICO notification, and while mandatory biometric data collection from thousands of students was ongoing. What changed in that update: a reference to the Strategic Portfolio Office was removed. Nothing else changed materially.

The Advocacy Policy — approved by the Safeguarding Steering Group — explicitly provides for disabled students to have their reasonable adjustments accommodated. There is no evidence this framework was applied to the deployment of remote invigilation in domestic environments or to the non-disclosure of alternative assessment arrangements to disabled students.

The governance failures documented in this case study did not occur in the absence of a governance framework. They occurred within one. The framework's existence did not prevent the failures. Its repeated updating did not address them. The problem is not the absence of policy. It is the absence of independent verification that policy is being followed.

Interim Conclusion — End of Part I

This case study has documented systematic governance failures in the deployment of remote invigilation software at a major UK university. Every finding is grounded in the institution's own documents, statutory FOI responses, and official records. No claim depends on assertion alone.

The failures reveal a structural gap in the regulatory architecture that allows high-risk biometric technologies to be imposed on students — including children aged 16 and 17 — without adequate safeguards, independent oversight, or enforceable remedies. The institution deployed a platform its own governance documentation told it not to deploy. The body that administered the procurement contract had a direct financial incentive, tied to utilisation, in the platform's continued adoption. The data protection regulator acknowledged non-compliance and closed the case. The complaints body is funded by the institutions it adjudicates. The quality regulator is gated behind the complaints body.

This is not the failure of one institution. It is the failure of a system.

Consider the full chain of assurance failure that this case study documents, starting from the SOC 2/AICPA conflict established in Section 4 and following it downstream to the sub-processor failures already documented in Section 3: the undisclosed Radius Global Solutions breach, and the OP360/iQor expansion into six non-adequate countries with no student notification and no Article 28(2) authorisation. At every node in this chain: no independent verification, no student disclosure, no UK adequacy protection, no functioning assurance mechanism. The unverified SOC 2 claim at the top of the chain means there was never any independent assurance that the sub-processor obligations flowing down it were being

met. A degree accredited by the body that governs the standard. A standard cited but never verified. Sub-processors in six non-adequate countries. A ransomware breach affecting 632,204 records. An unsigned governance document that reads, in its Information Asset Register field: “Link don’t work.” This is the full picture. It should not be allowed to happen again.

SOC 2 certification is a private standard set by a private membership organisation. There is no public registry of certified companies, no regulator who can verify a certificate independently, and no enforcement body if a claim is false. The only verification mechanism is the audit report itself — a private document the vendor chooses whether to share. The Open University never obtained that report. This is the equivalent of accepting a medical practitioner’s self-reported qualification without checking the GMC register — except that no GMC register exists for EdTech. One should exist.

The same conflict identified in Section 4 bears repeating in one sentence, because it is the sharpest fact in the whole chain: the body whose name was used to help sell the degree — AICPA & CIMA — is the same body whose standard was cited but never verified, and whose licensed auditors are now under investigation for fabricating the reports that constitute the only verification mechanism that standard provides. A widely cited industry summary of this arrangement describes it as a feature: “Since the AICPA & CIMA body both provides the professional qualifications and sets the security standards, it ensures a high level of data integrity and security for the exams you take through platforms like Meazure Learning.” That characterisation should be weighed against the evidence presented in this case study.

This matters beyond the individual case. Section 4 has already set out the scale of the Delve scandal; the point worth adding here is what happened after it broke. The AICPA has since actioned Accorp Partners — one of the certification mills named in that scandal — through its own peer review programme, finding that Accorp’s policies did not “provide reasonable assurance that engagement teams acted appropriately.” That is the AICPA’s own language for a firm alleged to have signed off on hundreds of pre-written SOC 2 reports. Despite that finding, Accorp Partners remains publicly operational, actively marketing SOC 2 and ISO 27001 services to new clients, with no public record of suspension or disciplinary action. A failed peer review triggers a private remediation process, not a public enforcement action. The industry operates, as one analyst put it, on a pure trust model: if you claim an AICPA-accredited auditor, no one verifies. No link between Meazure Learning and the implicated firms is alleged. The structural point stands: the OU cited a standard it never verified, administered by a body whose oversight failed at the precise moment those mechanisms were under active public scrutiny for systemic failure.

PART II — NEW EVIDENCE (April–July 2026)

Section 10: The University's Own Written Admission — Consent Is Not Freely Given Where No Alternative Exists

The University did not need to be caught. It told Parliament the rule itself.

In May 2026 the University submitted its own written evidence to this same Committee (reference AIE0218, contact Louis Trupia-Melluish). Paragraph 16 states, in the University's own words:

"Consent is another option but raises issues about validity, particularly for younger students or where no genuine alternative to AI-enabled services exists… Consent would not be regarded as 'freely given' where people have no real choice and should not therefore be relied on."

Read that twice. This is not an outside lawyer's theory of Article 7(4). It is the University's own statement of when consent fails — submitted in its own name, to Parliament, as guidance for how the sector should be regulated.

Now apply it. The University's own Help Centre states there is no alternative to an online invigilated examination for the modules at issue — public, live, unchanged. The platform vendor's own Terms of Service make acceptance a condition of entry: "You are not authorized to access or use the Site unless and until you accept these Terms," with no route to decline and still sit the exam — also public, also unchanged.

No real choice. No alternative. Consent given anyway, and relied on anyway. The University wrote the test. The University's own public documents fail it. This case study does not ask anyone to referee a contested reading of GDPR. It asks that the University be held to the standard the University itself proposed.

The facts, restated as the syllogism they are. Major premise, in the University's own words, published to Parliament: consent obtained where no genuine alternative exists is not freely given, and should not be relied on. Minor premise, in the University's own published Help Centre policy: no alternative exists for the modules at issue. Conclusion, unavoidable on the University's own terms and the University's own public documents: consent obtained under that policy was not freely given.

The major premise is not only the University's own; it is also the regulator's, and it predates the deployment. The ICO's own published guidance on biometric data, current from 15 April 2025 — four months before the September 2025 examinations this case study examines — states in terms: "You must offer a suitable alternative to people who choose not to consent. Otherwise, people do not have a real choice." The same guidance specifically flags the risk for institutions like the University: "This is

particularly an issue for public authorities… anyone who depends on your services, or fears adverse consequences if they refuse, may feel they have no choice but to agree." The University's own written position to Parliament a year later restates a standard its own sector regulator had already published, in similar terms, before a single student sat the exams at issue.

Secondary finding — equality impact assessment. The same evidence states, at paragraph 33: "There is currently no sector-wide standard for equality impact assessment in the adoption of AI in education… Institutions are making significant procurement and deployment decisions without consistent guidance on how to evaluate whether AI tools serve all their students fairly." Read alongside Part I, Section 5 — which documents, from FOI2026/023, that a disability-based alternative to the same platform was granted in every recorded case where a disabled student formally requested one — this is the University's own acknowledgement, in general terms, of the absence of the kind of structured equality analysis that would be needed to justify that differential treatment on a principled rather than ad hoc basis.

Section 11: The Personal-Data Delivery Reversal

The University was asked a direct question and gave a narrow answer designed to survive scrutiny without answering it. It took a second, contested disclosure round to get the truth.

A phishing incident (internal reference 2026-173) was identified internally on 1 April 2026 and reported to the ICO the next day. The University's own disclosures confirm 36,000 students and staff were targeted; 16,615 students received the email.

A subsequent FOI request (FOI2026/088) asked whether any mechanism existed by which the University delivers emails to students' personal, non-institutional email addresses. The University's initial response denied any such mechanism, but the denial was scoped narrowly to Outlook account forwarding only. Following an internal review, a further response (FOI2026/109, answered 1 July 2026 by a different named officer) reversed this position: the University confirmed that it "operates systems that deliver emails to students['] registered personal email addresses," that the personal address is added by the originating system automatically at the point of dispatch as a designed feature (not an incidental fault), and that those systems were active on 1 April 2026 — the date of the phishing incident.

The same FOI response further confirmed that no written Article 33 threshold assessment (the statutory assessment of whether a personal data breach must be notified to the regulator) exists for this incident at all — directly contradicting an earlier FOI response (FOI2026/066) which had stated that such an assessment was "completed" on 2 April 2026. The University's position is now that the threshold decision was "implicit" from

the fact that notification was in fact made, and was informally “explored” with the internal information-security function without being documented.

This sequence is not a technicality. First: no mechanism exists. Then, under pressure: yes, one exists, and it was built to work this way. Then, on the question of whether the University even checked whether the law required it to tell the regulator: no assessment exists, and the earlier claim that one had been “completed” was false. Three questions, three answers, three reversals — each only after the first answer was challenged. This is not how a governance function tells the truth the first time. It is how one is compelled to.

Section 173 of the Data Protection Act 2018 makes it an offence to alter, deface, block, erase, destroy, or conceal information with the intention of preventing its disclosure following a data subject’s exercise of their access rights. This case study does not allege that offence: nothing in the public record establishes intent, and intent is the element the statute requires. What the public record does establish is the sequence above — a statutory assessment represented as “completed” that, on the University’s own later account, never existed in writing, disclosed only after a contradictory earlier answer was challenged. Whether that sequence falls within Section 173, or is capable of being investigated as such, is a question for the Information Commissioner, not a finding this case study makes.

Section 12: The State Bar of California’s Settlement With Meazure Learning — and What Isn’t Settled

One lawsuit against Meazure Learning has ended. Others have not.

Part I referred to the State Bar of California’s amended complaint against Meazure Learning, filed 11 March 2026. That specific case concluded on 13 July 2026: Meazure Learning agreed to pay $5,250,000 in cash and waive $1,360,000 in outstanding invoices — $6.61 million combined, settled without admitting liability.

Read what the State Bar’s own complaint alleged before that settlement was reached. Fraudulent inducement and concealment. False promise. Negligent misrepresentation. Breach of contract. Breach of the implied covenant of good faith and fair dealing. Punitive damages were sought — conduct pleaded at the level of fraud or malice, not ordinary negligence. The State Bar’s own account states that discovery showed Meazure Learning “was making false promises it knew it was unable to deliver on,” and that it “deliberately hid information from the State Bar” about platform failures a November 2024 test run had already surfaced, months before the platform collapsed at scale during the February 2025 examination. Meazure Learning’s own employees raised internal doubts as early as September 2024 — the same month the University at the centre of this case study

began deploying the same platform, from the same vendor, for mandatory high-stakes UK assessment.

That settlement resolves one lawsuit. A second, separate action has since resolved too. Perjanik et al. v. ProctorU, Inc. d/b/a Meazure Learning — filed 27 February 2025 as Case No. 3:25-cv-02095 (N.D. Cal.) on behalf of a nationwide class of approximately 5,600 February 2025 California Bar Exam takers, later consolidated with two related actions and proceeding as 4:25-cv-02095-JST before Judge Jon S. Tigar — alleged breach of express and implied warranty, violation of California's Song-Beverly Consumer Warranty Act and Consumer Legal Remedies Act, unfair competition, unjust enrichment, and negligent infliction of emotional distress, arising from the same platform collapse. A motion for preliminary settlement approval was filed 18 September 2026: a reported $1.35 million resolution covering a 4,100-member class, a minimum $153 refund per claimant, up to $450,000 in attorneys' fees, roughly $28,000 in mediation and administration costs, and $10,000 incentive payments to each of seven named plaintiffs. Meazure Learning's spokesperson stated the company "vigorously defended against the claims and continues to deny any liability or wrongdoing," but "agreed to a settlement to avoid the time, expense and distraction of protracted litigation," adding that it "proudly stands behind" a record of "reliably administering over 4 million exams annually" over more than 20 years. The same vendor whose platform this case study documents as mandatory for UK students has now settled, without admitting fault, two separate US actions alleging it knew its platform could not do what it promised. None of that history has been shown to have been disclosed to the UK students required to use the same platform.

The settlement's data-handling terms are, separately, a useful benchmark. Meazure Learning was required to transfer scheduling and registration data, examination responses, proctor communications, support tickets, and examination video recordings to the State Bar, and thereafter to use "reasonable efforts" to permanently delete its own copies within 21 days, except where law requires retention (Part I, Sections 2 and 3, on retention and sub-processor governance). This shows what a sophisticated institutional client was able to negotiate for data return and deletion. The University's own arrangements, by comparison, remain undisclosed.

What California's own state auditor found — and what it didn't. A California State Auditor report (2025-051, published 9 July 2026) examined the February 2025 exam-day collapse and found the root cause to be the State Bar's own poor implementation planning. The auditor did not audit or interview Meazure Learning. The claim that circulated in media coverage — that students saw each other's answers — does not appear anywhere in the auditor's own report.

What the report does establish, in the State Bar's own contemporaneous records: Meazure Learning blamed the exam-day failure on an AWS outage at its hosting provider. The State Bar checked AWS's own public status page and found no record of any outage that day. Meazure Learning "provided no evidence" to support the claim. Separately, Meazure Learning's contract admitted, at signing, that its platform could not deliver a highlighting function the performance-test portion of the exam required — a third-party tool was not even contracted until four days before the exam, and was not integrated until the day before the mock sittings. More than two-thirds of the post-exam survey respondents reported copy-paste failures; about half reported highlight and strikethrough failures. And months before any of it, in September 2024, Meazure Learning told the State Bar it had run 25,000 test-takers through the platform in a single two-day period with no issues — the same month it was separately being onboarded, without independent verification, by the University at the centre of this case study.

Section 13: The Vendor's Own Current Documentation

Read what the vendor promises itself, in writing, and compare it to what students are told.

Terms of Service (last updated 6 May 2026). Meazure Learning disclaims any warranty that its own platform "will be accurate, reliable, error-free, or uninterrupted." It disclaims liability for equipment or network malfunction during a test-taker's session. And it makes acceptance non-negotiable: "You are not authorized to access or use the Site unless and until you accept these Terms" — no route to decline and still sit the exam. Disputes now go to binding individual arbitration under Virginia law, jury trial and class relief waived. An earlier version of the same Terms, obtained separately, had none of that: no arbitration clause, Alabama law, a different registered address again. Students already enrolled were moved from ordinary civil jurisdiction into binding US arbitration with no apparent specific notice that it had happened.

It gets worse. As of the most recent check, the University's own Help Centre still serves students the old version — the one without the arbitration clause, under the superseded law. The document a UK student is sent to when they want to understand what they've agreed to is not the document that actually governs them.

Privacy Policy — what quietly disappeared between November 2025 and May 2026. A capture of Meazure Learning's Privacy Policy from November 2025, compared directly against the version live on 6 May 2026, shows two changes that were never announced as changes. First: the November 2025 version pledged, in terms, that "Meazure does not sell, lease, trade, or otherwise profit from individuals' biometric data." That

sentence is gone from the May 2026 version. Nothing replaces it. Second: the November 2025 version's own CCPA disclosure chart stated the company does "not collect… racial or ethnic origin" from test-takers. The May 2026 version reverses this outright, adding racial and ethnic origin to a newly created "Sensitive Personal Information" category. A company does not accidentally start collecting a special category of data it previously told the public it did not collect. The same May 2026 update quietly adds tracking pixels and, for the first time, an explicit denial that the company engages in automated decision-making with legally significant effects — alongside the AI-training disclosure for support-chat content examined in full, against the Department for Education's own product safety standard, in Section 3 above. Whether that denial is accurate is a question this case study does not resolve. What it establishes is that the company added it, in the same update that removed a promise not to profit from biometric data and reversed a denial about collecting racial data. The State Bar of California settlement (13 July 2026) came after this policy change; the original lawsuit (filed 5 May 2025) and the amended complaint (11 March 2026) both came before it.

Data Processing Addendum and Standard Contractual Clauses. The vendor's own DPA states plainly that the data transferred includes "video images revealing racial or ethnic origin, biometric data, health data." It says biometric data is deleted "instantaneously," and other recordings after one year — a fraction of the three-year retention the University's own governance documents claim (Part I, Section 4). Two documents, one vendor, two different answers to "how long do you keep this." Separately, the vendor's own Standard Contractual Clauses page — the page its own compliance hub names as the actual legal mechanism for moving this data across borders — still runs on transfer clauses issued under a regulation repealed in 2018, superseded by the EU's 2021 framework, with a compliance deadline that passed in December 2022. More than eighteen months overdue. Uncorrected through the entirety of the State Bar of California litigation and settlement described in Section 12.

Two current University documents, one question, two different answers. The University's own Online Invigilation Policy states that "Meazure Learning's Privacy Notice supersedes The Open University's privacy notice for any audio and video footage or screen capture taken during the exam." The University's own Help Centre page on exam day says the opposite for the same recordings: they will be "kept in accordance with the Student Privacy Notice" — the University's, not the vendor's. Both pages were live on the same day this was checked. This is not one page going stale while another was updated. It is two currently-published University documents disagreeing, right now, about which organisation is legally responsible for a student's own recorded data.

This is not merely a transparency lapse. The Court of Appeal held, in Dale Vince v Associated Newspapers Ltd [2026] EWCA Civ 899 (15 July 2026), that a misleading juxtaposition of content can itself amount to unfair processing of personal data under UK GDPR Article 5(1)(a) — even where a fuller, accurate document exists elsewhere — because the court is entitled to take judicial notice that readers do not reliably read past the material actually placed in front of them. A student who encounters only the Help Centre page, or only the Policy, is materially misled about which entity governs their own recorded data. On that authority, this is an independent, live, current unfair-processing claim in its own right — not a documentation gap to be tidied up at leisure.

Section 14: The University's Own IT Department, in Its Own Words

Forget what the University told the regulator. Read what its own IT unit wrote down when nobody outside the building was meant to see it.

A Business Impact Assessment — BIA-460, authored by the University's own IT unit, disclosed nearly two months late under FOI — is the internal document that actually underpins the ProctorU rollout. Its own "additional comments" field admits: a prior BIA had already been completed before this one — this was a second attempt; an unresolved platform-level connection failure meant the University "cannot be sure that the ProctorU links will reliable [sic] work on any OU module"; and Meazure Learning's own personnel were granted access to the University's virtual learning environment specifically to diagnose that unfixed bug — all of this recorded as having happened before live students sat a single exam.

Seven admissions follow, each in the deploying unit's own words, none volunteered anywhere else:

"Uses AI? Unsure." The unit responsible for deploying the platform did not know whether it used AI. This sits directly against the University's repeated written denials elsewhere that any AI is used at all.

"Where is the data processed? UK." A third answer to a question the University's own DPQ files have already answered twice, inconsistently: USA in the original 2022 DPQ (GOV-1), Frankfurt in both versions of the March 2026 update. Now UK, from the unit that actually deployed the system.

Special category data, admitted as processed: health and disability information "indirectly," through proctors' awareness of extra-time accommodations; and ethnicity and political or religious indicators, through webcam observation of a student's own home. This is the University's own IT unit describing, in writing, the collection of Article 9 special category data with no legal basis recorded anywhere in the same document.

Four compliance checkboxes — GDPR enforcement tracker, ICO or other registration, international transfers, a breach check — marked as required and left blank. The “date responded to unit” field is blank too.

Students and staff are described as “wanting” to use ProctorU. Voluntary language, from an internal IT document, sitting directly against the University’s own public Help Centre stating there is no alternative.

ACCA accreditation is cited as the reason the platform had to be deployed at all: “if we don’t do it, we will lose accreditation.”

And the scope. BIA-460’s own approved pilot covered five modules. The University’s public mandatory list covers nine. No governance document establishes that the expansion beyond the approved pilot was ever itself approved.

None of this is disputed interpretation. It is the deploying unit’s own file, obtained under statute, describing what it did not know, could not confirm, and did not check — before mandating the platform for thousands of students.

PART III — GOVERNANCE AND PROCUREMENT (August 2026)

Parts I and II documented the deployment itself. Part III turns to the governance and procurement context around it: who sat where, who signed what, what risk categories were never built, and what the vendor of the remote-access software actually holds today by way of independent assurance.

Section 15: McCracken, Bain Capital, and Gryphon

Robert McCracken is OU’s Treasurer and chairs the Finance and Investment Committees. His Register of Interests entry discloses paid contractor roles at Fedrigoni SPA, Fox (Holdco) BV, and Maesa Expansion SAS.

Fedrigoni is a Bain Capital portfolio company. Maesa Expansion SAS is a Bain Capital portfolio company. MKM Building Supplies Ltd — a fourth McCracken role — sits on Bain Capital Private Equity’s own published portfolio list. McCracken chairs the Audit & Risk Committee at Fedrigoni, one of four Bain Capital companies where he holds paid governance roles.

Bain Capital Credit financed Gryphon Investors’ buyout of Meazure Learning/ProctorU in December 2020 and January 2021. Gryphon owns Meazure. Meazure is the vendor OU deploys against students’ exams.

Bain Capital Credit and Bain Capital Private Equity are separate divisions of one parent, Bain Capital LLC. McCracken's employer did not finance the Gryphon deal directly.

Julia Goodfellow, Vice-Chair of Council, sits on the same committees. She discloses a family member at Abingworth LLP, owned by Carlyle Group. A second private-equity adjacency on the same table.

The question is whether Governance and Nominations ever assessed this adjacency. Nothing in the public record shows that it did.

Note: Fox (Holdco) BV remains unverified against any Bain Capital entity after two search passes — not relied on above. Next step if pursued: Dutch KVK company register (kvk.nl).

Section 16: Who Signed the Meazure Contract

Financial Regulation 3.2.4 names five roles authorised to sign OU contracts: the Vice-Chancellor, the University Secretary, the Group Finance Director, the Head of Contract Services, and the Contracts Manager — or a person the Group Finance Director approves.

The Schedule of Financial Delegations that sets the actual approval thresholds is dated 30 November 2020. It predates ProctorU by nearly four years. It names roles, not thresholds — the pound-figure limits sit in a separate, unpublished appendix.

No document on the public record names who signed the Meazure contract, under what delegated authority, or at what spend threshold. The Chief Information Officer and the Director of Academic Services are the two roles whose remit most plausibly covers this decision. Neither is confirmed.

Section 17: No Category for Data Protection

OU's Responsible Procurement Strategy sets out the categories it uses to flag high-risk purchases. Data protection and privacy do not appear among them.

The strategy claims to cover all high-risk purchases. A biometric surveillance vendor, mandated across multiple cohorts, processing facial recognition and voice data transferred to the United States, does not trigger a category built for exactly that kind of risk — because no such category exists.

This is not a claim that Meazure's procurement bypassed a check. It is a claim that no check was ever built for this kind of risk.

Section 18: GoTo/LogMeIn — A Current Certificate, A Narrower Gap

This section concerns a different assurance gap from the Meazure SOC 2 failure documented in Sections 4 and 4A above. The vendor here is GoTo — the remote-access sub-contractor whose software runs the invigilation session — not Meazure Learning itself.

GoTo Group, Inc. is LogMeIn, rebranded in 2022. GoTo supplies LogMeIn Rescue, the remote access software used to invigilate students' exams — including the September 2025 examinations at the centre of this case. Rescue is a distinct GoTo product from GoTo Resolve, the product named in the NCC-CSIRT-2025-025 advisory cited in Section 1 above; that advisory does not describe Rescue and is not relied on in this section.

GoTo holds ISO 27001 certification, cert MMIND-25093001, issued by Mastermind Assurance LLC. Held continuously since 26 July 2019, reissued 24 April 2026. Scope names LogMeIn Rescue.

GoTo also holds a SOC 3 report covering 1 May 2025 to 30 April 2026, issued 9 July 2026. Scope names Rescue. The report's trust criteria are Security, Availability, and Confidentiality. Privacy is not among them.

The report does not assess whether GoTo's processing of personal data complies with data protection law. It assesses whether GoTo's systems are secure, available, and kept confidential. These are different questions.

What the Security, Availability, and Confidentiality trust criteria leave unexamined is visible in GoTo's own published Rescue Administrator Guide. The product can be configured to "automatically start as Windows System Service" where "the customer has administrative rights" — the remote-access applet installed on a student's personal device during an exam can, on GoTo's own documentation, be set up with elevated, persistent, system-level status rather than running only for the duration of the session. The same guide's timeout documentation states that "a value of 0 means an active session will never time out" and that certain processes — "an open remote control, screen sharing, or file manager session" among them — will themselves "prevent time out" from occurring at all. Taken together, these are GoTo's own stated architectural facts: the software supports both indefinite non-expiry and elevated installation, as configured features, not as faults. Whether either was active in any given OU invigilation session is not addressed by anything in this case study's record, including this section; what the SOC 3 report does not do is certify that neither was in play, because Privacy is not among the criteria it tests. On a related point, the same guide states that chat logs from a session are "deleted 24 hours from the moment they are queued for deletion" once an operator queues that deletion — a short, operator-controlled retention window for one of the few human-readable records a student would otherwise have of what occurred

during remote access to their device, and one more category the Security/Availability/Confidentiality scope has nothing to say about.

PART IV — REGULATORY SILENCE AND PUBLIC DATA (September–October 2026)

Parts I through III documented the deployment itself, what came to light in its aftermath, and the governance and procurement structure around it. Part IV turns to what the sector's own regulators say about themselves, in their own words and their own published data, when asked directly.

Section 19: The Information Commissioner's Office — No Framework Exists

Asked directly, in writing, whether it holds any policy, guidance, or briefing for assessing complaints that special category or biometric data has been collected by third-party remote invigilation vendors in higher education, the Information Commissioner's Office gave an unambiguous answer: "We do not hold information within scope of your request." No framework exists, anywhere within the regulator, for the specific category of harm this case study documents. This is a different, and more fundamental, gap than the one documented in Part I, Section 7: that section showed the regulator does not properly process the individual breach notifications it receives; this section shows it has never built a framework for assessing this category of complaint in the first place.

That admission sits against a sector-wide pattern the same regulator's own published casework datasets make visible. Across the 2025/26 financial year, the Information Commissioner's Office completed 544 data protection complaints against UK higher education providers under the "Higher education" sub-sector category of its own published casework datasets. 459 of those — 84.4 percent — were closed "No Further Action." Not a single decision notice, reprimand, or enforcement action was issued against any UK higher education institution under this heading in the same period. 336 of the 544 — 61.8 percent — were coded under Article 15, the right of access, as their primary reason: a category that captures a request for a copy of one's own data, not an assessment of whether the underlying collection was lawful in the first place. Only one of the 544 was coded under Article 9, the article governing biometric and other special category data — and that single case did not concern remote invigilation at all.

This is not evidence that biometric surveillance complaints in higher education are rare. It is consistent with, and plausibly explained by, the regulator's own admission above: a complainant who writes to the ICO to say, in effect, "I want to see what data was collected on me" is coded by a caseworker into whatever administrative category is the closest fit —

overwhelmingly Article 15 — because no dedicated category exists for the underlying substance of what they are actually describing. A regulator with no framework for assessing a harm has, by construction, no data recording that harm as what it is.

The Open University itself appears nine times in the same 544-case dataset, in the same period. Eight were closed "No Further Action." The ninth — received 6 November 2025 — was coded as an infringement under Article 15(3)(1), the right to a copy of one's own personal data, and resolved through informal action rather than formal enforcement. None of the University's nine cases in this dataset was coded as a biometric or special category matter.

Section 20: The Office for Students — Regulator and Commissioning Client

The Office for Students regulates the Open University's financial viability and sustainability under Condition D of its registration. In May 2022, the OfS also used its statutory validation powers under section 50 of the Higher Education and Research Act 2017 — for the first time — to commission the Open University as its national delivery partner for a three-year, government-funded validation project, worth up to £10 million, offering validation services to further education colleges seeking to deliver Level 4 and 5 courses. To formalise the commissioning terms, the OfS imposed a specific ongoing registration condition on the Open University under section 6 of the same Act — Condition BA — expressly stating that the condition "does not relate to the OU's compliance with its ongoing conditions of registration." That sentence does more than scope Condition BA narrowly: it is the OfS's own instrument recording that its commercial commissioning relationship with the Open University is to be treated, by its own design, as administratively separate from its ongoing regulatory conditions — including Condition D, under which the same regulator polices the same institution's financial viability. Whether that stated separation was accompanied by any corresponding operational separation — distinct teams, reporting lines, or decision-makers — is precisely what Items 3 and 4 of the FOI request described below sought to establish, and precisely what the Department's Section 12 refusal has, so far, left unanswered.

The same regulator is therefore, at the same time, a funder and commissioning client of the institution whose financial viability it is separately charged with policing. The OfS itself publicly evaluated and promoted this partnership on 27 May 2026, describing the project as testing "how the OfS could take a more active role" in the sector it regulates — in the same period the Open University's own audited financial statements record two consecutive years below its own stated 120-day liquidity floor (117 days at 31 July 2024; 109 days at 31 July 2025), and a £25.0 million Student Loans Company balance-sheet netting restatement.

Parliament has separately and independently examined the OfS's financial oversight in this same period. The House of Commons Public Accounts Committee found the Department for Education "not effectively holding the Office for Students to account" on systemic, sector-wide financial risk. The House of Lords Industry and Regulators Committee concluded, in its own words: "It is vital that regulators not only act with an appropriate degree of independence from the Government, but that they are perceived as doing so. This is evidently not the case for the OfS, where there is a widespread perception among providers, students and other stakeholders that it is not sufficiently independent."

None of this shows that the OfS's commissioning relationship with the Open University caused it to relax its scrutiny of the University's finances. No document establishes that, and this case study does not assert it. What the primary record does establish is a structural conflict of interest: the same regulator funding and publicly promoting a flagship national delivery partnership with an institution it is simultaneously responsible for holding to account on financial viability — a documented structural fact, not a proven instance of regulatory forbearance.

A Freedom of Information request to the Department for Education, seeking the underlying funding determination, pre-award due-diligence, and internal-separation records for this arrangement, was filed on 4 September 2026 (Ref: 2026-0087959). On 2 October 2026 the Department refused the request in full under Section 12(1) of the Freedom of Information Act 2000, stating that it could not confirm whether it holds the requested information because determining this would exceed the statutory cost threshold of £600 (3½ working days), and that, following its own guidance on multi-part requests, it does not sever and partially process individual items once the estimate for the whole exceeds that limit — notwithstanding that the request had expressly invited the Department to sever any item that did so and process the remainder. No search log, sampling exercise, or breakdown of the estimate was provided. The Information Commissioner's own published guidance on Section 12 requires that an authority's cost estimate be "reasonable" and supported by an actual assessment — which repository or directorate was checked, how many records that search would touch, and the time-and-motion basis for the figure reached — rather than a bare assertion that the threshold is exceeded; the refusal letter supplies none of this for a request confined, on its own Items 1 and 2, to two named categories of centrally held, statutory governance instrument. Under its separate Section 16 duty to advise and assist, the Department's own refusal identified, by name, the categories of document it regarded as capable of being supplied within the cost limit: "the principal funding or grant-allocation instrument" and records concerning "the original selection and funding decision." This is, in substance, the Department confirming that a narrower request for the primary grant determination and the selection

decision is a request it is equipped to answer — the same two instruments sought, among broader material, in Items 1 and 2 of the original request.

A refined request confined to those two instruments — the primary grant-allocation instrument and the ministerial or Senior Civil Service determination approving the Open University's selection — was submitted the same day, 2 October 2026, adopting the Department's own suggested scope verbatim and expressly excluding correspondence, drafts, and working notes to keep the request within the cost limit. That refined request remains outstanding as of this version, with a statutory response due by 30 October 2026. A request for internal review of the original Section 12 refusal, preserving the procedural record on the broader request, is also outstanding as of this version.

Implications

Taken together, the evidence in Parts I through IV points to gaps that recur across the case rather than sitting in any one finding: procurement bodies that are not structurally separated from the assurance function meant to check their own decisions; biometric data held to a lower evidentiary and retention standard than routine financial authentication; sub-processor chains that change without student notice or documented authorisation; internal risk assessments that identify a blocking problem and are overridden rather than resolved; disability-based exceptions granted case by case with no published criteria; a governance structure in which contract-signing authority, procurement risk categories, and board-level financial adjacencies are either undocumented, incomplete, or unassessed; a complaints architecture — university, adjudicator, and regulator alike — in which each body can point to another without any of them applying the standard the institution itself has, in writing, already conceded; and, at the level of the regulators themselves, a data protection regulator that admits, in writing, holding no framework for assessing this category of harm at all, and a financial regulator that is, concurrently, a commissioning funder of the very institution whose finances it is meant to police.

None of these gaps required new law to close. Existing UK GDPR, Consumer Rights Act, and Equality Act obligations already reach most of what this case study documents. What is missing is not the rule but the mechanism that tests conduct against it — before deployment, not after a student has already sat the exam.

Conclusion

Part I showed that a major UK university deployed a mandatory biometric surveillance platform for high-stakes assessment against its own governance documentation's explicit warnings, through a procurement structure with an undisclosed financial conflict of interest, without

independent security verification, and without disclosing sub-processor risk, disability alternatives, or safeguarding requirements affecting minors. Part II shows that the same university has separately told Parliament, in its own words, the precise legal test under which the consent obtained from those same students would be invalid — a test its own public Help Centre policy fails on its own terms — while its own internal IT department had already admitted, in writing, that it did not know whether the platform used AI at all. Part III shows that the governance structure sitting above all of this — who is authorised to sign the contract, what risk categories procurement is built to catch, and what adjacencies exist between the University's own office-holders and the investment group whose credit division financed the vendor's ultimate owner — has never itself been documented as assessed. Part IV shows that the principal data protection regulator holds no framework for assessing this category of harm at all, and that the principal financial regulator was, in the same period it was auditing the University's liquidity, also its commissioning funder for a separate national project — a structural conflict of interest neither regulator has been required to explain. The Department for Education's own refusal, on cost grounds, of the request for the underlying funding and due-diligence records illustrates the same point from a different angle: the documents that would show whether that conflict was ever formally managed are not, on the Department's own account, readily to hand.

This case study does not ask anyone to accept a contested legal argument on trust. The institution under scrutiny has already conceded the argument, in writing, to Parliament. What remains is the gap between that concession and its own conduct — documented here, in full, with its own words as the evidence.

Consolidated Evidence References

Part I sources (April 2026)

- FOI2026/023 — disability alternatives and completion rates — WhatDoTheyKnow
- FOI2025/238 — Open University, request for the ProctorU DPIA, response dated 28 October 2025 (Daniel Webb, Senior Manager Information Rights) — confirms "DPQ is the name used for DPIAs at the OU" — WhatDoTheyKnow
- FOI2026/032 — ProctorU use, DPQs, security assessments — WhatDoTheyKnow
- FOI2026/039 — SOC 2 compliance and data security — response received 26 March 2026 — no SOC 2 attestation report held

- FOI2026/044 — B252/B253 outcome data — response received 26 March 2026 — data discrepancy with FOI2026/023 under formal review
- FOI2026/083 — Open University — confirms the University holds no internal record of ProctorU examination sittings independent of the live third-party system — WhatDoTheyKnow
- 1EdTech TrustEd Apps Directory — Meazure Learning / ProctorU search, verified 27 March 2026
- Meazure Learning compliance page — meazurelearning.com/compliance — GDPR link misattribution verified 27 March 2026
- NCC-CSIRT Advisory NCC-CSIRT-2025-025 (Nigeria Communications Commission CSIRT, csirt.ncc.gov.ng) — HIGH/HIGH classification for LogMeIn/GoTo Resolve abuse as a malware-delivery vector. Not a JISC publication; cited independently, not as evidence of JISC's own knowledge. Concerns GoTo Resolve, not GoTo Rescue — see Part III, Section 18.
- Government Cyber Action Plan — January 2026 — gov.uk
- UK Government Fraud Strategy 2026–2029 — published 9 March 2026 — gov.uk
- Jisc news release, "Cyber-attacks against UK education and research are growing more complex and sophisticated," 26 February 2026, summarising findings from the annual cyber threat intelligence report (full report restricted to Jisc's cyber security community group) — jisc.ac.uk
- iQor acquisition of OP360 — GlobeNewswire — 5 January 2026
- Meazure Learning Privacy Policy, "Last Updated: May 6, 2026" — Cookies and Other Tracking Technologies / Website Delivery and Appearance section — discloses that chat-based support interaction data "may be used by Zendesk… to help train and improve Zendesk's AI systems" — meazurelearning.com
- Department for Education, "Generative AI: product safety standards," published 19 January 2026 — gov.uk — addressed to edtech developers and suppliers to schools and colleges
- California State Bar amended complaint against Meazure Learning — filed 11 March 2026, Los Angeles Superior Court

- Active class action litigation against Radius Global Solutions, following its 2023 MOVEit/Clop ransomware breach — ongoing
- Full FOI response and attached DPQs (the original DPQ is referred to throughout this case study as GOV-1): https://www.whatdotheyknow.com/request/use_of_proctoru_remote_proctorin#incoming-3351760
- "ProctorU DPQ Updated March 2026" (Assessment, Risk Assessment, Questionnaire, and AI/ML tabs) — the March 2026 update to GOV-1, disclosed under FOI2026/039 — source for the Individual Rights/Security "partially met" entries and the Assessment tab's "Artificial Intelligence, Machine Learning or Algorithms usage are not part of this activity" entry, both quoted in Section 4
- Letter to a named OU student re MST125 assessment arrangements, signed Richard English, Student Casework Manager, Tuition, Assessment, Curriculum and Quality (TACQ), dated 22 March 2026 — shared publicly by the recipient with express consent for reuse as evidence

Part II sources (April–July 2026)

- ICO guidance, biometric data, current from 15 April 2025 — ico.org.uk — predates the September 2025 examinations; states organisations "must offer a suitable alternative to people who choose not to consent," with a worked example naming public authorities specifically
- AIE0218 — Open University written evidence to the Education Committee, "The Use of Artificial Intelligence and EdTech in Education," dated May 2026, contact Louis Trupia-Melluish. Published at committees.parliament.uk (search reference AIE0218 within work/9642 written evidence).
- Oral evidence transcript, HC 151, 7 July 2026, Panel I (Witnesses: The King's Trust, Institute for the Future of Work, Nuffield Foundation, British Chambers of Commerce) — https://committees.parliament.uk/oralevidence/17949/pdf/
- Oral evidence transcript, HC 151, 7 July 2026, Panel II (Witnesses: University College London, Purposeful Ventures, Oak National Academy, Monash University) — https://committees.parliament.uk/oralevidence/17951/pdf/
- FOI2026/066 — Open University, phishing incident 2026-173 — breach scope and initial (later superseded) Article 33 assessment claim

- FOI2026/088 — Open University, personal-address mail delivery mechanism — initial narrow denial
- FOI2026/109 — Open University, response of 1 July 2026 — reversal confirming personal-address delivery mechanism operates by design; confirms no written Article 33 threshold assessment exists
- ICO internal review, Case Reference IC-524089-W4X7, dated 31 July 2026 — confirms the ICO does not record an outcome category at initial assessment of an Article 33 breach notification, does not record any verification of the notification's factual accuracy, and does not record follow-up on accuracy or completeness; internal review upheld the original response without addressing its substance
- ICO published guidance, "Understanding and assessing risk in personal data breaches" — ico.org.uk — sets out the seven-step documented risk-assessment methodology the ICO requires of data controllers, compared against IC-524089-W4X7 above
- Business Impact Assessment BIA-460, Open University IT unit — disclosed under FOI, nearly two months late
- California State Auditor Report 2025-051 (Auditor Grant Parks, published 9 July 2026) — root-cause findings on the February 2025 exam-day collapse; explicitly does not assess or reach conclusions on the State Bar's litigation against Meazure Learning
- Dale Vince v Associated Newspapers Ltd [2026] EWCA Civ 899, Court of Appeal, 15 July 2026 — unfair processing under UK GDPR Article 5(1)(a) via misleading juxtaposition
- State Bar of California v. Meazure Learning, Case No. 25STCV13089, Superior Court of Los Angeles County — executed Settlement Agreement, 13 July 2026
- California State Bar public statements on the amended complaint and settlement — calbar.ca.gov
- Federal class action against Meazure Learning, consolidated N.D. Cal., mediation before a retired federal judge — ongoing, not settled
- Perjanik et al. v. ProctorU, Inc. d/b/a Meazure Learning, originally filed as Case No. 3:25-cv-02095, N.D. Cal., 27 February 2025, nationwide class of approximately 5,600 February 2025 California Bar Exam takers; consolidated with two related actions and proceeding as 4:25-cv-02095-JST before Judge Jon S. Tigar — preliminary settlement approval motion filed 18 September 2026, reported $1.35 million resolution, 4,100-member class, $153 minimum refund per claimant (Legal Newsline, 1 October 2026)

- Meazure Learning Terms of Service — meazurelearning.com — version last updated 6 May 2026, compared against a pre-6-May-2026 version obtained separately
- Meazure Learning Privacy Policy — meazurelearning.com/privacy-policy — November 2025 capture (metadata: created 6 November 2025) compared against the version live 6 May 2026
- Meazure Learning Data Processing Addendum — meazurelearning.com/data-processing-addendum
- Meazure Learning Standard Contractual Clauses page — meazurelearning.com/standard-contractual-clauses — page metadata confirms last modification 16 December 2024
- Open University Online Invigilation Policy, section 2.4, and Open University Help Centre “On the day of the exam” page — help.open.ac.uk — both checked as live and current 30 July 2026
- Open University Help Centre — hosted copy of Meazure Learning Terms of Service — confirmed to be the pre-6-May-2026 version as of 28 July 2026

Part III sources (August 2026)

- Open University Register of Interests — Robert McCracken (Treasurer, Chair of Finance and Investment Committees) entry disclosing paid contractor roles at Fedrigoni SPA, Fox (Holdco) BV, Maesa Expansion SAS, and MKM Building Supplies Ltd
- Open University Register of Interests — Julia Goodfellow (Vice-Chair of Council) entry disclosing a family member’s role at Abingworth LLP (owned by Carlyle Group)
- Open University Council Constitution, updated 1 August 2026 — confirms the five contract-signing roles under Financial Regulation 3.2.4
- Open University Schedule of Financial Delegations, dated 30 November 2020
- Open University Responsible Procurement Strategy — current published version, checked for stated high-risk purchase categories
- Bain Capital Credit press release, 28 January 2021, baincapital.com — confirms senior credit facilities financing Gryphon Investors’ majority buyout of Meazure Learning/ProctorU

- Fedrigoni SPA governance page — confirms Fedrigoni as a Bain Capital portfolio company and McCracken's role chairing its Audit & Risk Committee
- Bain Capital Private Equity published portfolio list — confirms MKM Building Supplies Ltd
- US FTC HSR early-termination filing, Transaction 20191119 (Bain Capital Europe Fund V, SCSp), granted, dated approximately 15 April 2019 — confirms Maesa Expansion SAS as a Bain Capital portfolio company, corroborated by Bain Capital's own press release, 28 March 2019, and independent press coverage
- GoTo ISO 27001 certificate MMIND-25093001, Mastermind Assurance LLC — held continuously since 26 July 2019, reissued 24 April 2026, scope names LogMeIn Rescue
- GoTo Systems Management SOC 3 report, period 1 May 2025–30 April 2026, issued 9 July 2026 — scope names Rescue; trust criteria Security, Availability, Confidentiality (no Privacy category)
- GoTo/LogMeIn Rescue Administrator Guide (GoTo, Inc., published vendor documentation) — "Automatically start as Windows System Service" / administrative-rights configuration option; session timeout settings including indefinite non-expiry and the processes that prevent timeout; chat-log 24-hour post-queue deletion window

Part IV sources (September–October 2026)

- ICO Freedom of Information response, Case Reference IC-552138-Y2M7, 4 September 2026 — confirms the ICO holds no policy or guidance for assessing complaints involving special category or biometric data collected by third-party remote invigilation vendors in higher education
- ICO quarterly "Data protection complaints" casework datasets, financial year 2025/26 (Q1–Q4), ico.org.uk — downloaded and independently analysed directly
- Office for Students blog, "Building higher education pathways locally: Lessons from the OfS's validation project with the Open University," Alastair Wilson, 27 May 2026, officeforstudents.org.uk
- Office for Students, "Regulatory case report for the Open University – specific ongoing condition BA," officeforstudents.org.uk
- Higher Education and Research Act 2017, sections 5, 6, and 50 — legislation.gov.uk

- House of Commons Public Accounts Committee, “Financial sustainability of the higher education sector in England,” Eighth Report of Session 2022–23, HC 257, June 2022
- House of Lords Industry and Regulators Committee, “Must do better: the Office for Students and the looming crisis facing higher education,” HL Paper 246, September 2023, Chapter 8, paragraph 412
- Freedom of Information request to the Department for Education, “HERA 2017 Section 50 Commissioning, Regulatory Governance and Financial Monitoring,” filed 4 September 2026, Ref: 2026-0087959, WhatDoTheyKnow
- Department for Education, response to FOI request 2026-0087959, 2 October 2026 — refusal in full under Section 12(1) of the Freedom of Information Act 2000; no search log, sampling exercise, or cost breakdown provided; Section 16 advice identifying the principal grant-allocation instrument and the selection/funding decision as the categories of document the Department regarded as answerable within the cost limit
- Freedom of Information request to the Department for Education, “Level 4/5 Validation Project (The Open University) – Primary Grant Determination & Selection Instruments (Refined from Ref: 2026-0087959),” submitted 2 October 2026, WhatDoTheyKnow — outstanding as of this version, statutory response due by 30 October 2026

Every document cited above is a public record: a statutory FOI disclosure, a court or tribunal filing, a published government or regulatory report, or a vendor’s or institution’s own live web page or disclosed governance document.

Author: Valentina Bozhilova, MIAB

First drafted April 2026. This version: 2 October 2026.